

DUOを使用したISE 3.3ネイティブMulti-factor Authenticationの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[フロー図](#)

[コンフィギュレーション](#)

[保護するアプリケーションの選択](#)

[ISEとActive Directoryの統合](#)

[オープンAPIの有効化](#)

[MFAアイデンティティソースの有効化](#)

[MFA外部アイデンティティソースの設定](#)

[ユーザをDUOに登録](#)

[ポリシーセットの設定](#)

[制限事項](#)

[確認](#)

[トラブルシューティング](#)

はじめに

このドキュメントでは、Identity Services Engine(ISE)3.3パッチ1をMulti-factor AuthenticationのDUOと統合する方法について説明します。バージョン3.3パッチ1以降では、ISEはDUOサービスとのネイティブ統合用に設定できるため、認証プロキシは不要です。

前提条件

要件

次の項目に関する基本的な知識が推奨されます。

- ISE
- DUO

使用するコンポーネント

このドキュメントの情報は、次のハードウェアに基づくものです。

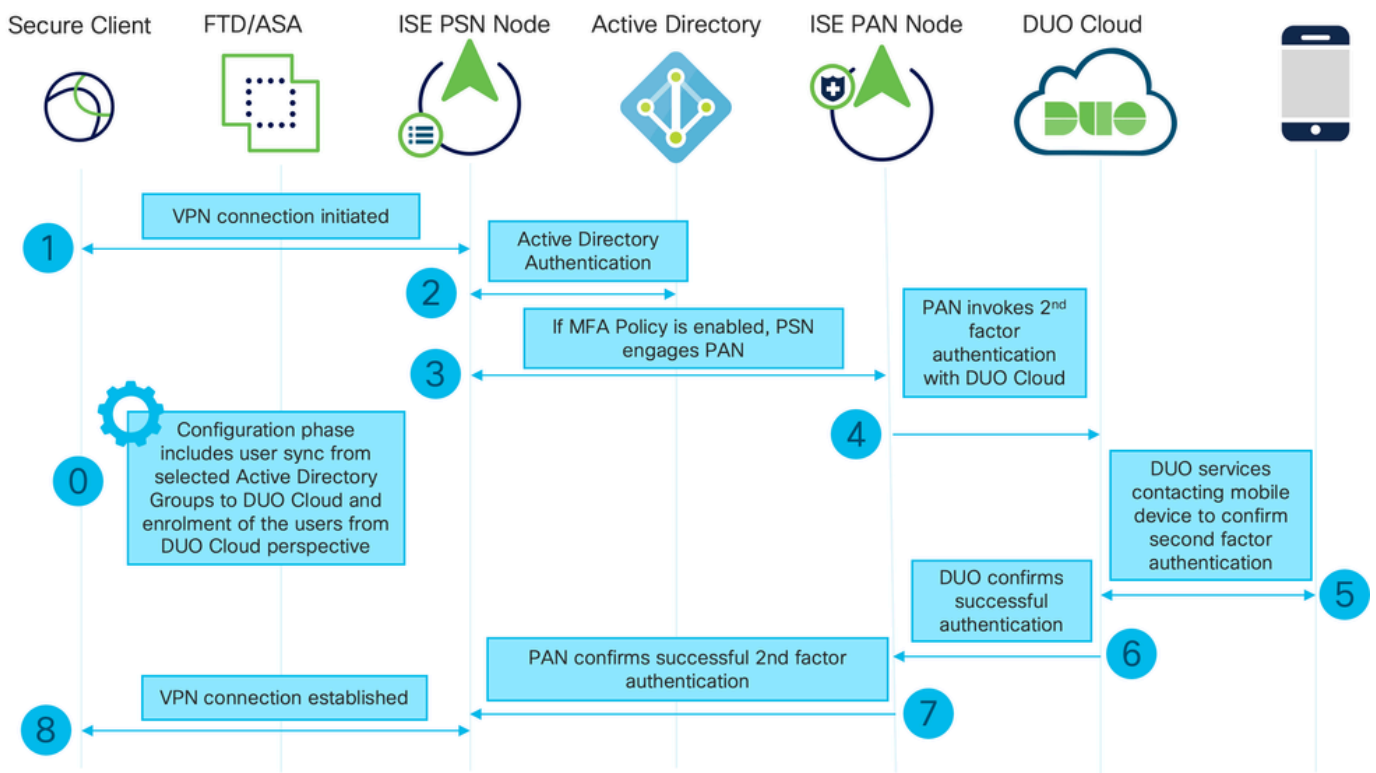
- Cisco ISEバージョン3.3パッチ1

- DUO
- Cisco ASA バージョン 9.16(4)
- Cisco Secure Clientバージョン5.0.04032

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

フロー図



フロー図

手順

0.構成フェーズにはActive Directoryグループの選択が含まれ、そこからユーザが同期されます。同期はMFAウィザードが完了すると行われます。この操作は、次の2つの手順からなります。Active Directoryを参照してユーザと特定の属性のリストを取得します。Admin APIを使用したDUO Cloudへの呼び出しは、そこにユーザをプッシュするために行われます。管理者はユーザを登録する必要があります。登録には、Duo Mobileのユーザーをアクティブにするオプションのステップを含めることができます。これにより、ユーザーはDuo Pushでワンタップ認証を使用できます

1. VPN接続が開始され、ユーザがユーザ名とパスワードを入力して「OK」をクリックします。ネットワークデバイスがRADIUS Access-RequestをPSNに送信

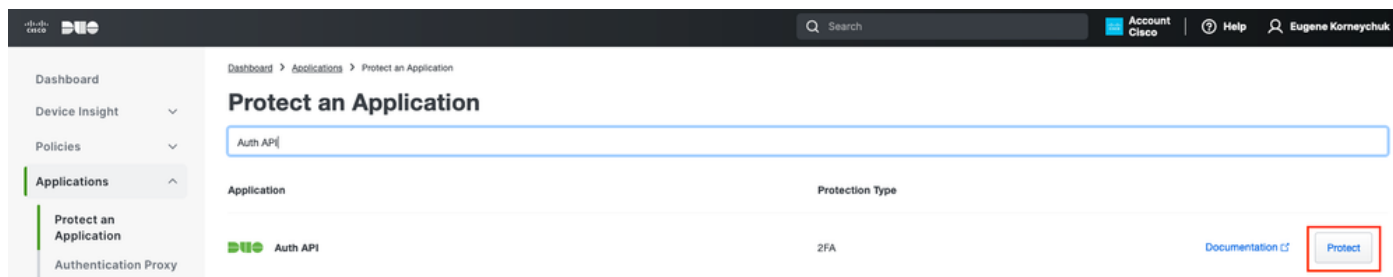
2. PSNノードがActive Directory経由でユーザを認証する
3. 認証が成功し、MFAポリシーが設定されると、PSNはDUO Cloudに接続するためにPANを開始します
4. DUO Cloud with Auth APIへの呼び出しは、DUOを使用した2段階認証を呼び出すために行われます。ISEはSSL TCPポート443でDuoのサービスと通信します。
5. 2番目の要素認証が行われます。ユーザが2番目の要素の認証プロセスを完了する
6. DUOは、第2要素認証の結果をPANに応答します
7. PANは、第2要素認証の結果をPSNに応答します
8. Access-Acceptがネットワークデバイスに送信され、VPN接続が確立されます

コンフィギュレーション

保護するアプリケーションの選択

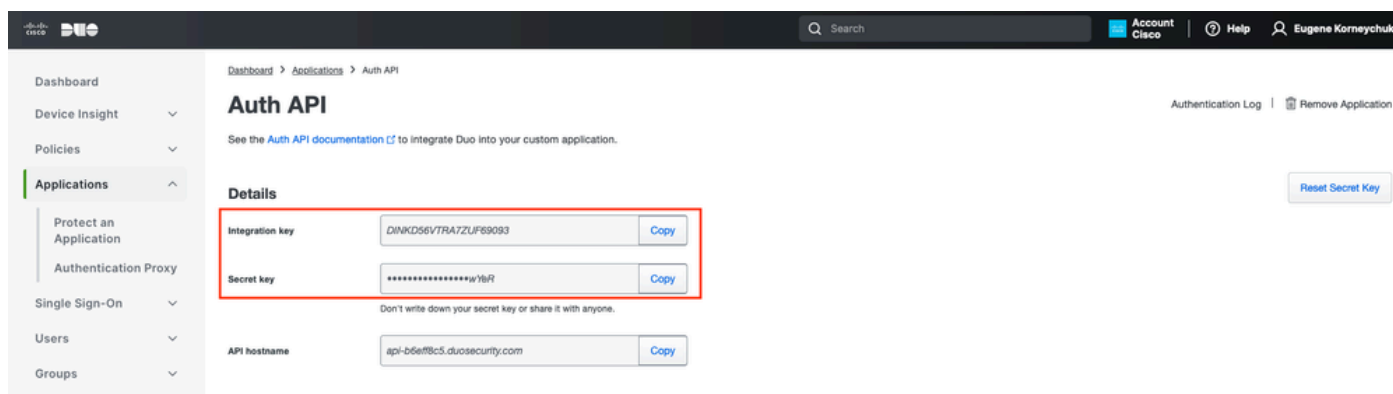
DUO Admin Dashboard <https://admin.duosecurity.com/login>に移動します。管理者クレデンシャルでログインします。

Dashboard > Applications > Protect an Applicationの順に移動します。Auth APIを探し、Protectを選択します。




認証API 1

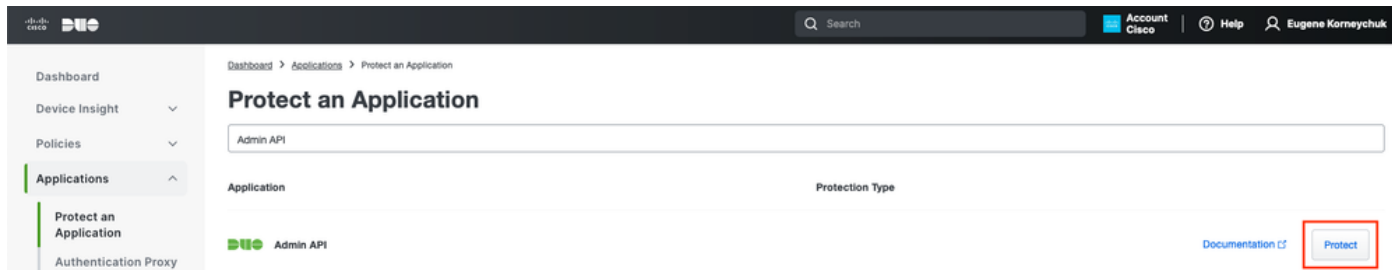
統合キーと秘密キーをメモします。



認証API 2

Dashboard > Applications > Protect an Applicationの順に移動します。Admin APIを探し、Protectを選択します。

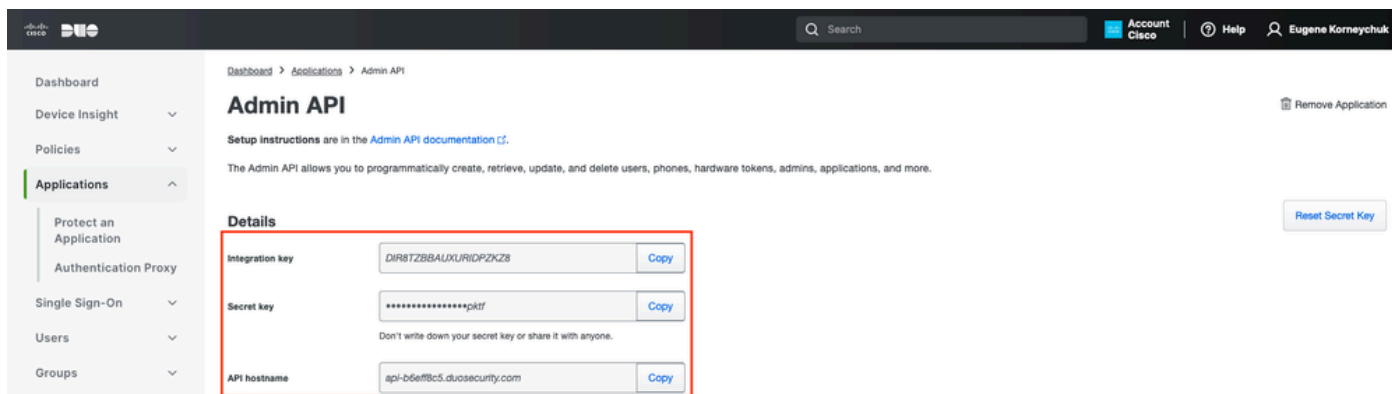
 注:Duo Admin PanelでAdmin APIアプリケーションを作成または変更できるのは、Ownerロールを持つ管理者だけです。



The screenshot shows the Duo Admin Panel interface. The breadcrumb trail is Dashboard > Applications > Protect an Application. The main heading is 'Protect an Application'. Below it is a search bar containing 'Admin API'. A table lists applications with columns for 'Application' and 'Protection Type'. The 'Admin API' entry is highlighted. To the right of the table, there are links for 'Documentation' and a 'Protect' button, which is highlighted with a red box.

認証API 1

統合キー、秘密キー、およびAPIホスト名をメモします。



The screenshot shows the 'Admin API' details page. The breadcrumb trail is Dashboard > Applications > Admin API. The main heading is 'Admin API'. Below it, there are setup instructions and a description: 'The Admin API allows you to programmatically create, retrieve, update, and delete users, phones, hardware tokens, admins, applications, and more.' A 'Details' section is highlighted with a red box, containing three fields: 'Integration key' with value 'DIR8TZBBAUXJRIDPZKZ8', 'Secret key' with value '*****pkzf', and 'API hostname' with value 'api-b6eff8c5.duosecurity.com'. Each field has a 'Copy' button. There are also 'Remove Application' and 'Reset Secret Key' buttons on the right.

管理API 2

API権限の設定

ダッシュボード>アプリケーション>アプリケーションに移動します。Admin APIを選択します。

Grant Read ResourceとGrant Write Resourceのアクセス許可にチェックマークを入れます。Save Changesをクリックします。

Groups ▾

Endpoints ▾

2FA Devices ▾

Administrators ▾

Trusted Endpoints

Trust Monitor ▾

Reports ▾

Settings

Billing ▾

You're using the new Admin Panel menu and left-side navigation.
[Provide feedback](#)

API hostname [Copy](#)

Settings

Type Admin API

Name

Duo Push users will see this when approving transactions.

Permissions

- Grant administrators
Permit this Admin API application to add, modify, and delete administrators and administrative units.
- Grant read information
Permit this Admin API application to read information and statistics generally used for reporting purposes.
- Grant applications
Permit this Admin API application to add, modify, and delete applications.
- Grant settings
Permit this Admin API application to read and update global account settings.
- Grant read log
Permit this Admin API application to read logs.
- Grant read resource
Permit this Admin API application to read resources such as users, phones, and hardware tokens.
- Grant write resource
Permit this Admin API application to add, modify, and delete resources such as users, phones, and hardware tokens.

管理API 3

ISEとActive Directoryの統合

1. Administration > Identity Management > External Identity Stores > Active Directory > Addの順に移動します。[Join Point Name] と [Active Directory Domain] に入力し、[Submit] をクリックします。

Identity Services Engine Administration / Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

External Identity Sources

- > Certificate Authentica...
- > Active Directory
- > MFA
- > Identity Sync
- > LDAP
- ODBC
- > RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login
- > REST

Connection

- * Join Point Name ○
- * Active Directory Domain ○

[Submit](#) [Cancel](#)

Active Directory 1

2. すべてのISEノードをこのActive Directoryドメインに参加させるプロンプトが表示されたら、Yesをクリックします。



Information

Would you like to Join all ISE Nodes to this Active Directory Domain?

No

Yes

Active Directory 2

3. ADのユーザ名とパスワードを入力し、OKをクリックします。



Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name ⓘ Administrator

* Password

Specify Organizational Unit ⓘ

Store Credentials ⓘ

Cancel


OK

Active Directory 3




ISEのドメインアクセスに必要なADアカウントは、次のいずれかを持つことができます。

- 各ドメインのドメインユーザ権限にワークステーションを追加する

- ISEマシンのアカウントがドメインに参加する前に作成される各コンピュータコンテナに対するコンピュータオブジェクトの作成またはコンピュータオブジェクトの削除の権限

 注：シスコでは、ISEアカウントのロックアウトポリシーを無効にし、誤ったパスワードが管理者に使用された場合にアラートを送信するようにADインフラストラクチャを設定することを推奨します。誤ったパスワードが入力されると、ISEは必要なときにマシンアカウントを作成または変更しないため、すべての認証が拒否される可能性があります。

4. ADのステータスはOperationalです。

Connection	Allowed Domains	PassiveID	Groups	Attributes	Advanced Settings
* Join Point Name	example				
* Active Directory Domain	example.com				
+ Join + Leave  Test User  Diagnostic Tool  Refresh Table					
<input type="checkbox"/>	ISE Node	ISE Node R...	Status	Domain Controller	Site
<input type="checkbox"/>	ise331.example.com	PRIMARY	<input checked="" type="checkbox"/> Operational	WIN2022.example.com	Default-First-Site-Name
<input type="checkbox"/>	ise332.example.com	SECONDARY	<input checked="" type="checkbox"/> Operational	WIN2022.example.com	Default-First-Site-Name

Active Directory 4

5. 「グループ」>「追加」>「ディレクトリからグループを選択」>「グループの取得」に移動します。次の図に示すように、選択したADグループ（ユーザの同期と許可ポリシーに使用）に対してチェックボックスをオンにします。

Select Directory Groups

This dialog is used to select groups from the Directory.

Domain example.com

Name *
Filter

SID *
Filter

Type
Filter ALL

Retrieve Groups... 50 Groups Retrieved.

<input type="checkbox"/>	Name	Group SID	Group Type
<input type="checkbox"/>	example.com/Users/Cert Publishers	S-1-5-21-4068818894-3653102275-25587130...	DOMAIN LOCAL
<input type="checkbox"/>	example.com/Users/Cloneable Domain Controllers	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input checked="" type="checkbox"/>	example.com/Users/DUO Group	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Denied RODC Password Re...	S-1-5-21-4068818894-3653102275-25587130...	DOMAIN LOCAL
<input type="checkbox"/>	example.com/Users/DnsAdmins	S-1-5-21-4068818894-3653102275-25587130...	DOMAIN LOCAL
<input type="checkbox"/>	example.com/Users/DnsUpdateProxy	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Domain Admins	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Domain Computers	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Domain Controllers	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Domain Guests	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Domain Users	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Enterprise Admins	S-1-5-21-4068818894-3653102275-25587130...	UNIVERSAL

Cancel

OK

Active Directory 5

6. Saveをクリックして、取得したADグループを保存します。

[Edit](#) [+ Add](#) [Delete Group](#) [Update SID Values](#)

<input type="checkbox"/>	Name	SID
<input type="checkbox"/>	example.com/Users/DUO Group	S-1-5-21-4068818894-3653102275-2558713077-...

[Save](#) [Reset](#)

Active Directory 6

オープンAPIの有効化

Administration > System > Settings > API Settings > API Service Settingsの順に移動します。
Open APIを有効にして、Saveをクリックします。

The screenshot shows the 'Administration / System' settings page in the Identity Services Engine. The 'Settings' tab is selected, and the 'API Settings' section is expanded. Under 'API Service Settings for Primary Administration Node', the 'Open API (Read/Write)' toggle is turned on and highlighted with a red box. Other settings like 'ERS (Read/Write)' and 'ERS (Read)' are also visible. At the bottom right, there are 'Reset' and 'Save' buttons.

オープンAPI

MFAアイデンティティソースの有効化

Administration > Identity Management > Settings > External Identity Sources Settingsの順に移動します。MFAを有効にして、Saveをクリックします。

Identity Services Engine Administration / Identity Management

Settings

External Identity Sources Settings

REST ID Store

To allow integration of REST identity stores with Cisco ISE, click the radio button below. It takes a few minutes to enable the REST ID Store settings. After the settings are enabled, you can add REST ID stores to Cisco ISE in the [External Identity Source](#) page.

NOTE: ISE integration with Azure AD is released as a Controlled Introduction feature and should be thoroughly tested before being used in production environment.

REST ID Store

Multi-Factor Authentication BETA

To allow the integration of Multi-Factor Authentication providers with Cisco ISE, click the MFA button.

MFA

Cancel

ISE MFA 1

MFA外部アイデンティティソースの設定

[Administration] > [Identity Management] > [External Identity Sources] に移動します。[Add] をクリックします。ウェルカム画面でLet's Do Itをクリックします。

Identity Services Engine Add External Connector

1 Welcome 2 Connector Definition 3 Account Configurations 4 Identity Sync 5 AD Groups 6 Summary

Welcome

This wizard takes you through setting up a connection between your Duo Account and Cisco ISE to enable seamless Multi-Factor Authentication workflows.

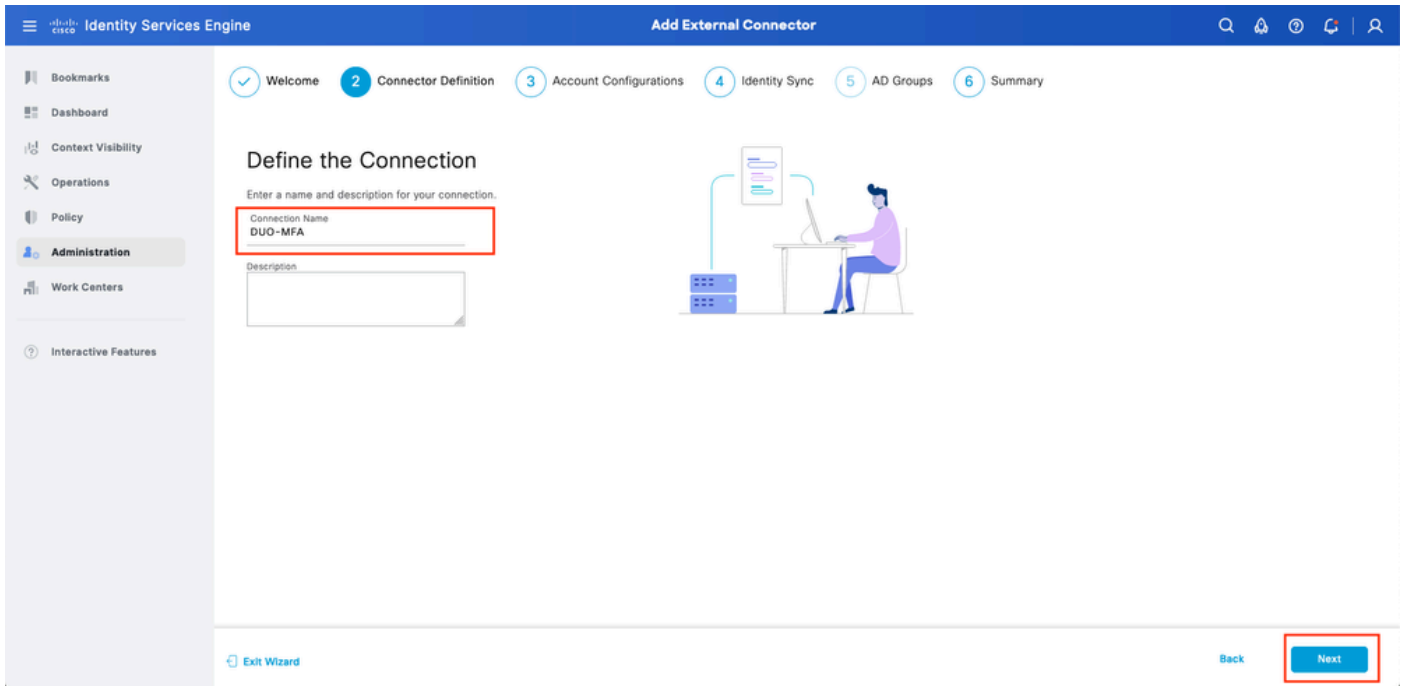
Before you begin, the following prerequisites apply:

1. Cisco ISE Advantage licenses are required.
2. The Cisco Duo license that enables MFA usage is required.
3. In your Duo portal, create a protected application that is enabled for Admin API and Authentication API usage.
4. Grant read/write access to Admin API.
5. Ensure your ISE has a stable connection to Duo (Either through direct internet or proxy).
6. For this application, note the integration keys (ikey), secret keys (skey) and API hostname values for the Admin and Authentication APIs. These values are required in the next steps of this setup wizard.

Exit Wizard

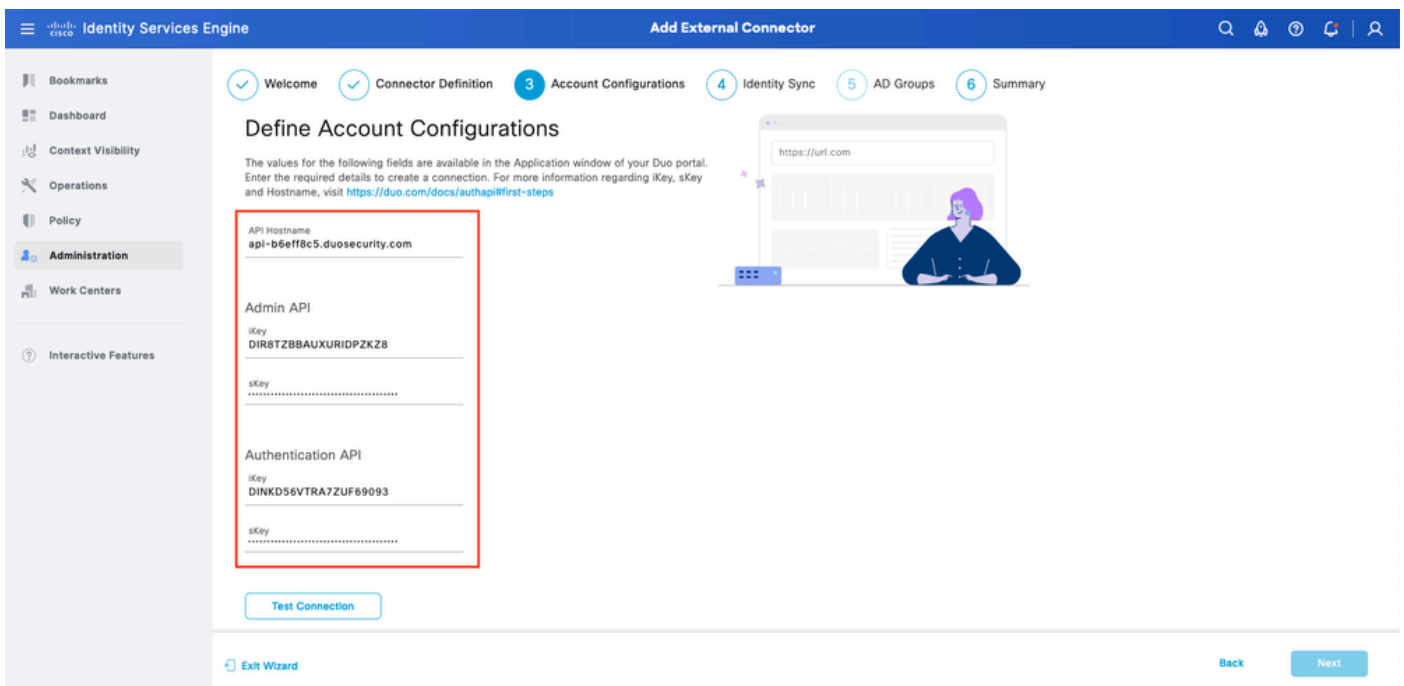
ISE DUOウィザード1

次の画面でConnection Nameを設定し、Nextをクリックします。



ISE DUOウィザード2

Select Applications to Protectステップで、API Hostname、Admin API Integration and Secret Keys、Auth API Integration、およびSecret Keysの値を設定します。




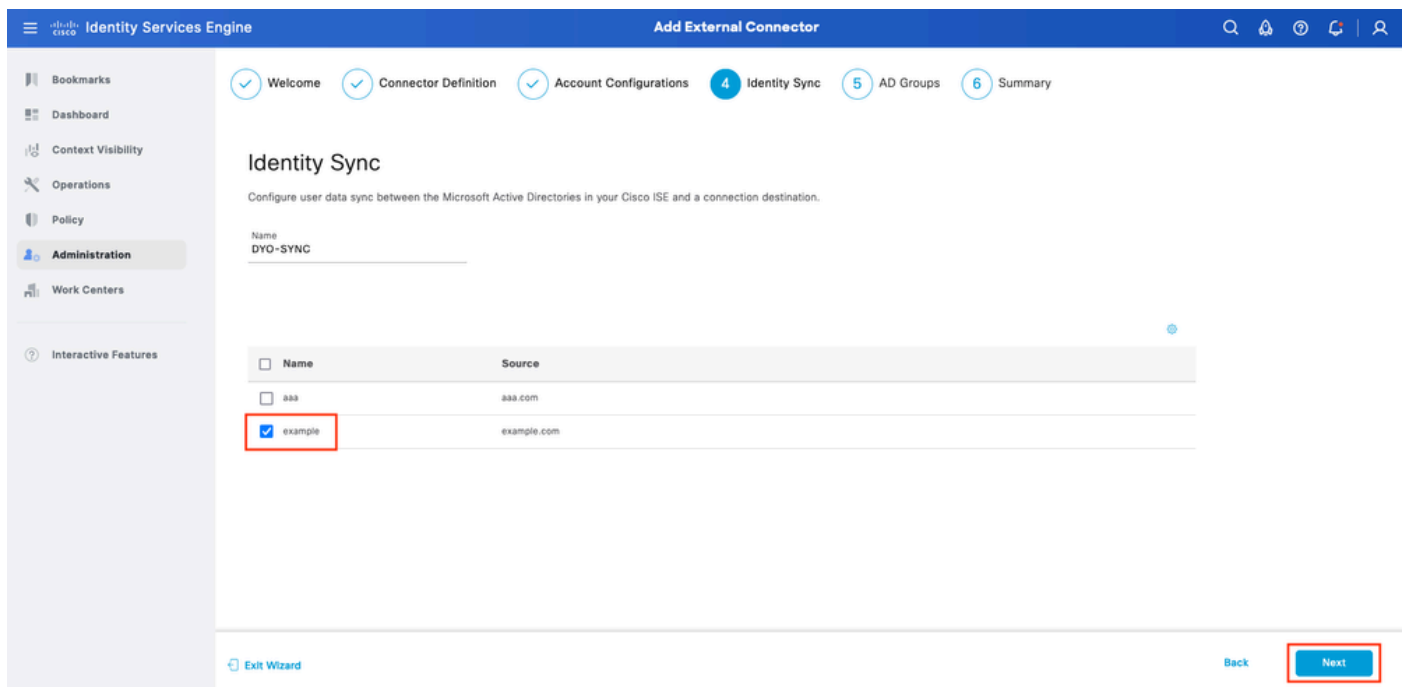
ISE DUOウィザード3

Test Connectionをクリックします。Test Connectionが成功したら、Nextをクリックします。



Identity Syncを設定します。このプロセスでは、選択したActive Directoryグループのユーザが、前述したAPIクレデンシャルを使用してDUOアカウントに同期されます。Active Directory Join Pointを選択します。[Next] をクリックします。

 注：Active Directoryの設定はこのドキュメントの対象範囲外です。ISEをActive Directoryと統合するには、この[ドキュメント](#)の説明に従ってください。



Identity Services Engine Add External Connector

Welcome Connector Definition Account Configurations **4 Identity Sync** 5 AD Groups 6 Summary

Identity Sync

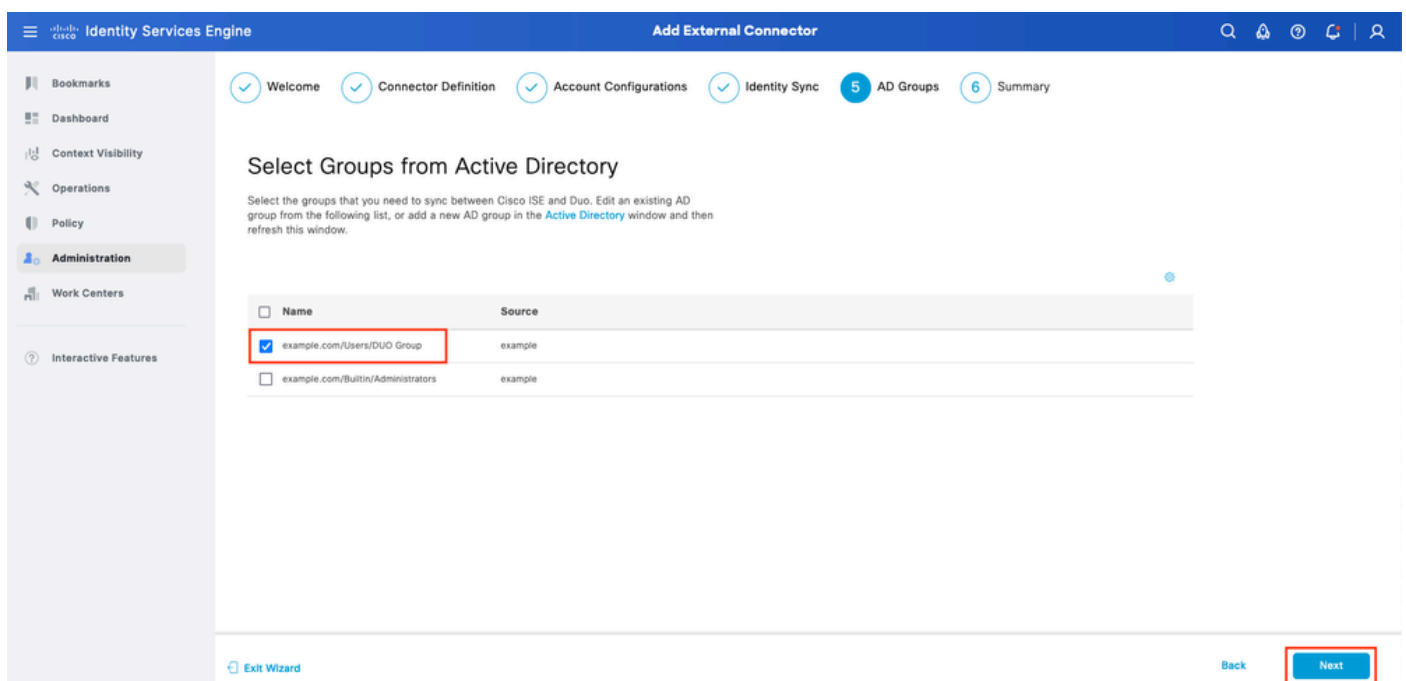
Configure user data sync between the Microsoft Active Directories in your Cisco ISE and a connection destination.

Name
DYO-SYNC

<input type="checkbox"/> Name	Source
<input type="checkbox"/> aaa	aaa.com
<input checked="" type="checkbox"/> example	example.com

Exit Wizard Back **Next**

ユーザをDUOと同期させるActive Directory Groupsを選択します。[Next] をクリックします。



Identity Services Engine Add External Connector

Welcome Connector Definition Account Configurations Identity Sync **5 AD Groups** 6 Summary

Select Groups from Active Directory

Select the groups that you need to sync between Cisco ISE and Duo. Edit an existing AD group from the following list, or add a new AD group in the Active Directory window and then refresh this window.

<input type="checkbox"/> Name	Source
<input checked="" type="checkbox"/> example.com/Users/DOU Group	example
<input type="checkbox"/> example.com/Builtin/Administrators	example

Exit Wizard Back **Next**

設定が正しいことを確認して、Doneをクリックします。

Identity Services Engine Add External Connector

6 Summary

Summary

Connector Definition [Edit](#)

Connection Name DUO-MFA

VPN

TACACS

Define Account Configurations [Edit](#)

API Hostname api-b6eff8c5.duosecurity.com

Authentication API

iKey DIR8TZBBAUXURIDPZKZ8

sKey

Admin API

iKey DINKD56VTRA7ZUF69093


sKey

Authentication MFA Auth and Admin API Integration and Secret Keys are valid

Identity Sync [Edit](#)

[Exit Wizard](#) [Back](#) [Done](#)

ユーザをDUOに登録

 注：DUOユーザ登録はドキュメントの範囲外です。ユーザの登録の詳細については、この [ドキュメント](#) を参照してください。このドキュメントの目的では、手動によるユーザ登録を使用します。

DUO Admin Dashboardを開きます。Dashboard > Usersの順に移動します。ISEから同期されたユーザをクリックします。

Dashboard > Users

Users

Directory Sync | Import Users | Bulk Enroll Users [Add User](#)

Need to activate a replacement phone? [Learn more about Reactivating Duo Mobile](#).

2 Total Users **1** Not Enrolled **1** Inactive Users **0** Trash **0** Bypass Users **0** Locked Out

Select (0) ... [Export](#) Search

Username	Name	Email	Phones	Tokens	Status	Last Login
<input type="checkbox"/> alice	alice	alice@wonderland.com	1		Active	Nov 14, 2023 1:43 AM
<input type="checkbox"/> bob	bob				Active	Never authenticated

2 total

DUO登録1

Phonesまでスクロールします。Add Phoneをクリックします。

Phones

You may rearrange the phones by dragging and dropping in the table. [Learn more about activating a replacement phone](#).

This user has no phones. [Add one.](#) [Add Phone](#)

DUO登録2

電話番号を入力し、電話の追加をクリックします。

Dashboard

Device Insight ▼

Policies ▼

Applications ▼

Single Sign-On ▼

Users ▲

Add User

Pending Enrollments

Bulk Enroll Users

Import Users

Directory Sync

Bypass Codes

Dashboard > Users > bob > Add Phone

Add Phone



[Learn more about Activating Duo Mobile](#)

Type Phone Tablet

Phone number

[Show extension field](#)

Optional. Example: "+1 201-555-5555"

Add Phone

ポリシーセットの設定

1. 認証ポリシーの設定

Policy > Policy Setの順に移動します。MFAを有効にするポリシーセットを選択します。プライマリ認証IDストアをActive Directoryとして使用して認証ポリシーを設定します。

Status	Rule Name	Conditions	Use	Hits	Actions
●	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	0	⚙️
●	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores > Options	1	⚙️
●	DUO Authentication	Radius-NAS-Port-Type EQUALS Virtual	example > Options		⚙️
●	Default		All_User_ID_Stores > Options	7	⚙️


ポリシーセット1

2. MFAポリシーの設定

MFAがISEで有効になると、ISEポリシーセットの新しいセクションが使用可能になります。MFA Policyを展開し、+をクリックしてMFA Policyを追加します。MFAの設定任意の条件で、DUO-MFAを選択します(前述のUseセクションで設定)。[Save] をクリックします。

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring Policy Sets. The main area displays a table of Policy Sets. The 'MFA Policy(1)' section is expanded, showing a table of rules. A rule named 'DUO Rule' is highlighted with a red box. The rule's conditions are 'Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS RA'. The rule's use is 'DUO-MFA'. The 'Options' button is also highlighted with a red box. The 'Save' button at the bottom right is also highlighted with a red box.

ISEポリシー

 注：上記で設定したポリシーは、RAという名前のトンネルグループに依存しています。RAトンネルグループに接続されたユーザは、強制的にMFAを実行します。ASA/FTDの設定は、このドキュメントの対象範囲外です。この[ドキュメント](#)を使用して、ASA/FTDを設定します

3.許可ポリシーの設定

Active Directoryグループの条件と任意の権限を使用して認可ポリシーを設定します。

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring Authorization Policies. The main area displays a table of Authorization Policies. The 'Authorization Policy(16)' section is expanded, showing a table of rules. A rule named 'DUO Authorization Rule' is highlighted with a red box. The rule's conditions are 'example-ExternalGroups EQUALS example.com/Users/DUO Group'. The rule's use is 'PermitAccess'. The 'Options' button is also highlighted with a red box.

ポリシーセット3

制限事項

このドキュメントの作成時点：

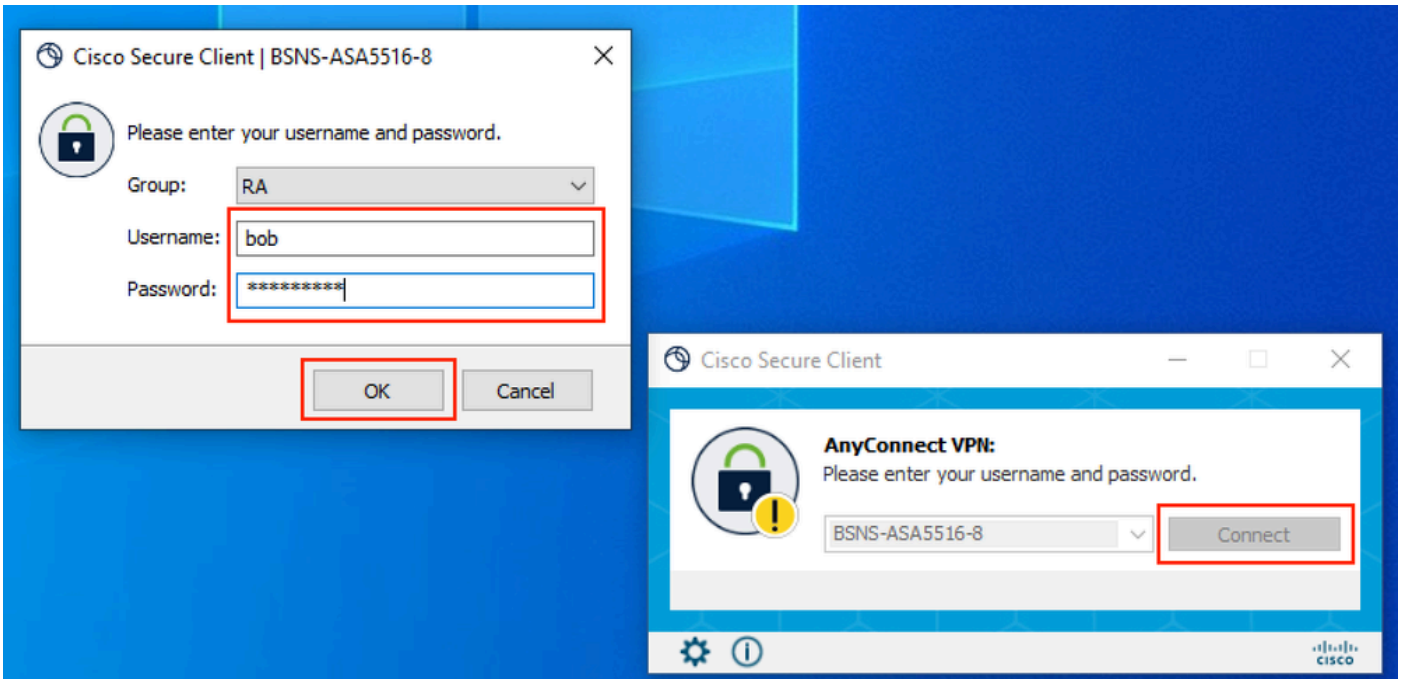
- 1.第2の認証方式としてサポートされているのは、DUOプッシュと電話だけです
2. DUO Cloudにプッシュされるグループはありません。ユーザー同期のみがサポートされます

3.次の多要素認証の使用例のみがサポートされています。

- VPNユーザ認証
- TACACS+管理アクセス認証

確認

Cisco Secure Clientを開き、Connectをクリックします。UsernameとPasswordを入力して、OKをクリックします。



VPN クライアント

ユーザのモバイルデバイスは、DUOプッシュ通知を受信する必要があります。承認します。VPN接続が確立されます。

1:52



Search

Accounts (8)

Add



Cisco
Cisco



Are you logging in to Auth API?

🌐 Cisco

🕒 1:52 PM

👤 bob

MFA関連のログ	ポリシーエンジン	ise-psc.log	DuoMfaAuthApiUtils -:::- Duo Client managerに要求を送信 DuoMfaAuthApiUtils → Duo応答
ポリシー関連のログ	prrt-JNI	prrt-management.logに保存します。	RadiusMfaPolicyRequestProcessor TacacsMfaPolicyRequestProcessor (オプション)
認証に関連するログ	ランタイムAAA	prrt-server.log (サーバのIPアドレス)	MfaAuthenticator::onAuthenticateEvent MfaAuthenticator::sendAuthenticateEvent MfaAuthenticator::onResponseEvaluatePolicyEvent
DUO認証、ID同期に関連するログ		duo-sync-service.log (サービスの二重同期ログ)	

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。